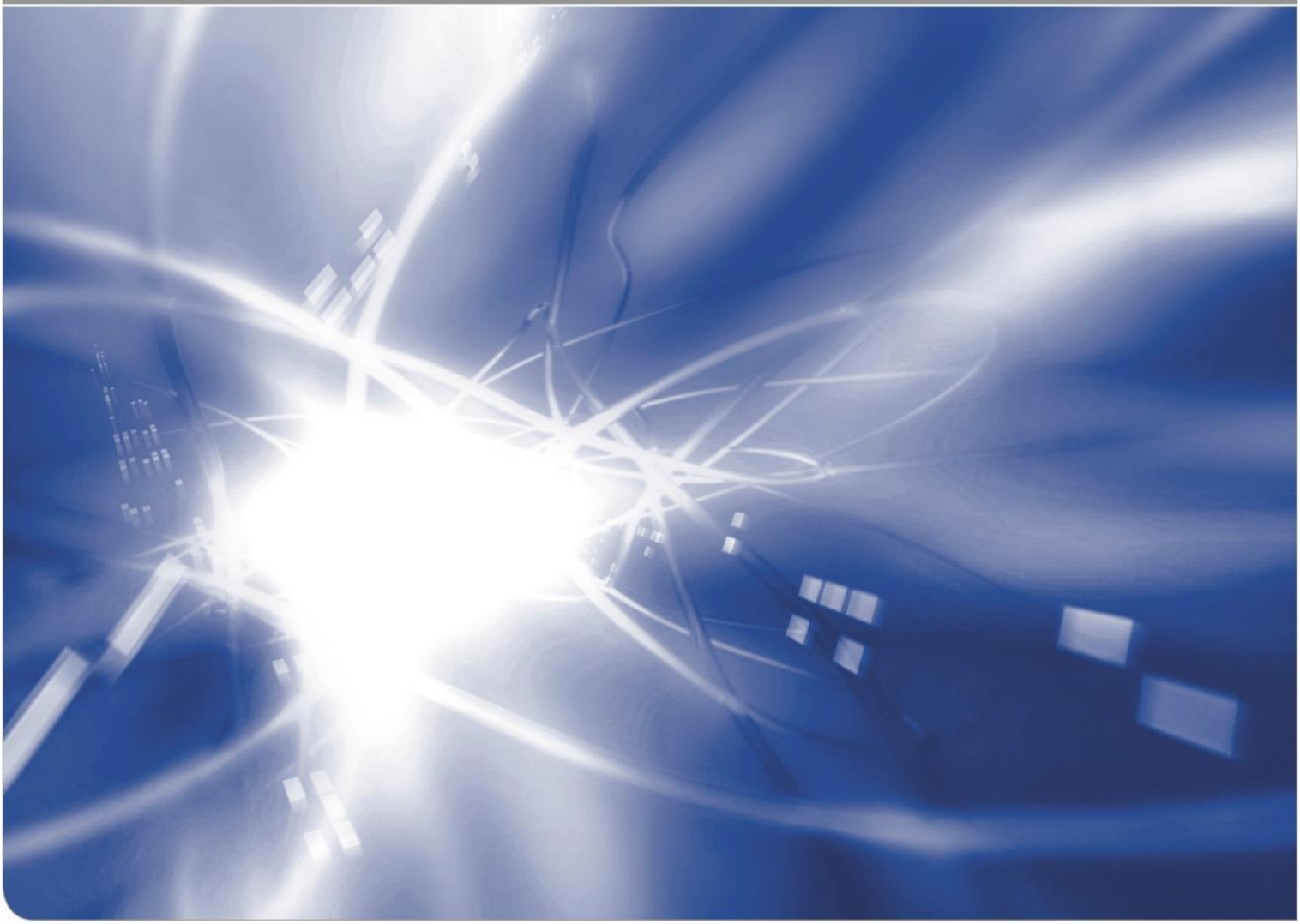
Karlsruher Institut für Technologie

Big Data – quo vadis?

Trends, Treiber, Determinanten, Wildcards

Von Oliver Siemoneit

KIT SCIENTIFIC WORKING PAPERS 86



Impressum

Karlsruher Institut für Technologie (KIT)
www.kit.edu

2018

ISSN: 2194-1629

Big Data, quo vadis?

Trends, Treiber, Determinanten, Wildcards

Dr. phil. Dipl.-Kfm. techn. Oliver Siemoneit
Institut für Technikfolgenabschätzung und Systemanalyse (ITAS)
Karlsruher Institut für Technologie (KIT), Karlstraße 11, 76133 Karlsruhe
(oliver.siemoneit@kit.edu)

ITAS ABIDA Arbeitspapier Nr. 1

Begleitforschung Big Data „ABIDA – Assessing Big Data“
(BMBF-Förderkennzeichen 01IS15016A-F)

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Kurzfassung

Am 25. Mai 2018 tritt die Datenschutz-Grundverordnung (DS-GVO) in allen EU-Mitgliedsstaaten in Kraft. Sie ist zentral für die rechtliche Regulierung des Einsatzes von Big-Data-Anwendungen mit Personenbezug im privatwirtschaftlichen Bereich. Das vorliegende Arbeitspapier untersucht in analytischer Absicht die Passung der Big-Data-Vision mit der DS-GVO. Die Identifikation von Stärken und Schwächen rechtlicher Regulierung bildet die Basis dafür, im Sinne einer juristischen Gesetzesfolgeabschätzung mögliche gesellschaftliche Ausprägungsformen des heutigen und vor allem künftigen Einsatzes von Big-Data-Technologien zu identifizieren, um ggfs. Handlungsbedarfe zu antizipieren. Die Darstellung unterschiedlicher Diskurspositionen (und den damit verbundenen Erwartungen, Hoffnungen, Ängsten) bietet ferner einen basalen Orientierungsrahmen, der die Möglichkeit für ein proaktives Risikomanagement eröffnet. Deutlich wird dabei, dass die DS-GVO eine Vielzahl von Vorzügen mit sich bringt, jedoch einige zentrale Aspekte des Einsatzes von Big Data – insbesondere im Bereich Profiling, Scoring und automatisierten Entscheidungen – nur unvollständig reguliert.

Danksagung

Ich danke Herrn Dr. Thilo Weichert für die Vielzahl wertvoller Anmerkungen – auch wenn die akademisch-distanzierte Diagnose von vermeintlichen Unfertigkeiten und Unzulänglichkeiten der DS-GVO bzw. die Benennung von Diskurspositionen nicht unbedingt zu seinem Kerngeschäft zählt.

Ein herzliches Dankeschön geht auch an Tristan Tillmann und Christian Straker, Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster für die kritische Durchsicht und Kommentierung des Manuskripts und an Julia Fuchs-Bechtel für das Lektorat.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BVerfG	Bundesverfassungsgericht
DS-GVO	Datenschutz-Grundverordnung
ePV	ePrivacy-Verordnung
EWG	Erwägungsgrund
GRCh	Charta der Grundrechte der Europäischen Union
IuK	Informations- und Kommunikationssysteme
UWG	Gesetz gegen den unlauteren Wettbewerb

1 Szenariomethode und mögliche Zukünfte

Die Zukunftsforschung versucht auf methodisch gesicherter Basis belastbare Aussagen über zukünftig mögliche Entwicklungen zu treffen. Mittels der sog. Szenariomethode werden systematisch Trends, Treiber und mögliche Diskontinuitäten identifiziert, die die Basis dafür abgeben, a) unterschiedliche Entwicklungswege als auch b) daraus resultierende alternative Zustände („Zukünfte“) zu identifizieren.[1] Die Szenariomethode setzt dabei sowohl unterschiedliche Kreativmethoden (Experten-Workshops, Zukunftswerkstätten etc.) als auch statistische Methoden (Trendextrapolation, Cross-Impact-Analysis, Störereignisanalyse etc.) ein.[2] Welche Methoden im Einzelnen verwendet werden, insbesondere welche Verfahren in Anschlag gebracht werden, um Zukunftsbilder/Szenarien auf Plausibilität und Konsistenz zu prüfen, unterscheidet sich zwischen den unterschiedlichen Ansätzen der Szenariomethode oft erheblich.[3] Gemeinsam ist allen Szenarioansätzen jedoch grob folgendes Phasenschema:[4]

1) Problemanalyse und Szenariofeldbestimmung: Zu welchem Zweck und für welche Zielgruppe sollen Szenarien entwickelt werden? Welchen thematischen Betrachtungsfokus sollen die Szenarien haben?

2) Identifikation von relevanten Schlüsselfaktoren: Welche Variablen, Parameter, Trends, Entwicklungen und Ereignisse sind für die zukünftige Entwicklung des zu betrachtenden Feldes relevant?

3) Schlüsselfaktoranalyse: Welche möglichen Entwicklungen können die unterschiedlichen Schlüsselfaktoren nehmen? Wie interagieren sie? Welche sind wichtigere, welche unwichtigere Schlüsselfaktoren?

4) Szenariogenerierung: Welche denkbare Entwicklung der unterschiedlichen Schlüsselfaktoren lassen sich in plausiblen, konsistenten Zukunftsbildern bündeln? Welche alternativen zukünftigen Zustände/Zukünfte ergeben sich hieraus?

Das vorliegende Arbeitspapier hat vor diesem Hintergrund das Ziel, erste Vorüberlegung für die Phasen 1 und 2 anzustellen, indem es sowohl alternative Betrachtungsschwerpunkte (Phase 1) als auch möglicherweise relevante Schlüsselfaktoren (Phase 2) kursorisch benennt. Das Arbeitspapier möchte damit nicht alternative, plausible und in sich konsistente Big-Data-Zukünfte entwerfen, sondern lediglich Gedanken dazu anstellen, was a) relevante Themen für unterschiedliche Zielgruppen sein könnten und b) in welche Richtung Entwicklungen gehen könnten, indem zentrale Trends und Treiber, Stellhebel, Ursachen und Gründe für mögliche Diskontinuitäten identifiziert und benannt werden. Zentral hierfür ist neben der Analyse unterschiedlicher Diskurspositionen sozialer Akteure v. a. die Analyse des existierenden Rechtsrahmens, der den Einsatz von Big-Data-Lösungen mit Personenbezug maßgeblich reguliert und determiniert: die europäische Datenschutz-Grundverordnung (DS-GVO) und das novellierte Bundesdatenschutzgesetz (BDSG-neu).

[1] Vgl. Steinmüller (1997), S. 50ff.
[2] Vgl. Steinmüller (1997), S. 59ff.
[3] Vgl. Steinmüller (1997), S. 59ff.
[4] Vgl. Steinmüller (1997), S. 60f. und Kosow/Gaßner (2008), S. 19ff.

2 Big Data als Reflexionsbegriff

Der Begriff „Big Data“ ist in den letzten Jahren zu einem zentralen Schlagwort in wissenschaftlichen, politischen und gesellschaftlichen Diskursen avanciert, unter dessen Dach einschneidende Veränderungen der Digitalisierung – deren Chancen als auch Risiken – kontrovers diskutiert und zwischen unterschiedlichen sozialen Akteuren verhandelt werden. Der Begriff „Big Data“ fokussiert dabei auf die Tatsache, dass moderne Informations- und Kommunikationstechnologien (IuK) es ermöglichen, auf einfache Art und Weise große Mengen an Daten zu erfassen, zu speichern, auszutauschen, zusammenzuführen und zu analysieren. Das Produzieren und Generieren von Daten ist dabei – zu einem gewissen Grad – den IuK-Technologien systeminhärent und unvermeidbar.[1] Neben der Erbringung des eigentlichen Grundservices für den Nutzer eröffnet dies meist die Möglichkeiten einer Mehrfachnutzung[2] der angefallenen Daten, was meist mit erheblichen Begehrlichkeiten von Werbeunternehmen, Strafverfolgungsbehörden, fremden Staaten, Cyber-Kriminellen etc. einhergeht. Nicht zuletzt basiert auch Big-Data-Analytics auf dieser Mehrfachnutzungsstrategie, indem Daten „auf Vorrat“ gesammelt und problemorientiert mit anderen Datenbestände ad-hoc kombiniert werden, um die Idee einer kybernetischen Gesellschaft zu realisieren.[3] Aus Sicht des Datenschutzes können dabei zwei grundlegende Arten von Big-Data-Analysen unterschieden werden.[4] Statistische Analysen auf dem Makrolevel abstrahieren durch Anonymisierung der Rohdaten von der Einzelperson und erlauben die Beantwortung von Fragen wie: Wo ist die beste Stelle für ein Wahlplakat? Wo die größte Wahrscheinlichkeit für einen Verkehrsunfall? Wie breiten sich Infektionskrankheiten aus? Big-Data-Analysen auf der Mikroebene hingegen dienen der Erkennung, Analyse und Beurteilung von Eigenschaften natürlicher Personen: Ist die Person zuverlässig genug, um einen Kredit zu gewähren? Wer der Wahlberechtigten ist noch unentschlossen und evtl. mit welchem Argument beeinflussbar? Welcher Nutzer kann welcher Werbebotschaft nicht widerstehen?

Insgesamt ist festzustellen, dass eine einheitliche, allgemein akzeptierte Definition des Begriffs „Big Data“ nicht existiert bzw. die Definition je nach Disziplin und Erkenntnisinteresse oft stark divergiert.[5] Für die vorliegende Untersuchung hat der Begriff „Big Data“ daher die Funktion eines Reflexionsbegriffes, unter dessen Dach problemorientiert verschiedene Facetten der Digitalisierung in kritischer Absicht beleuchtet werden sollen, um implizite Präsuppositionen und Hypostasierungen verschiedener sozialer Akteure zu explizieren und einer Diskussion zugänglich zu machen. Die dabei besonders interessierenden Facetten der Digitalisierung sind:

1) Die zunehmende massive Erfassung sowohl personenbezogener Daten als auch personenbeziehbarer Daten durch informatische Systeme.
2) Die Zusammenführung und Kombination unterschiedlichster Datenbestände und deren Analyse mittels statistisch-inferenzieller Verfahren.
3) Die Erörterung der gesellschaftlichen Folgen von Profiling und Scoring, von Predictive Analytics, Machine-Learning und automatisierten Entscheidungen.

[1] Vgl. Türpe et al. (2016).
[2] Zur herausragenden Bedeutung der Untersuchung der Mehrfachnutzung von Technologien im Rahmen der Technikethik siehe Liebert (2013).
[3] Vgl. Pentland (2014).
[4] Vgl. Roßnagel 2013, S. 562.
[5] Siehe hierzu exemplarisch die Vielzahl disziplinärer Definitionen bzw. die zweckabhängige Erweiterung der klassischen 3-Vs-Definition in Kolany-Raiser et al. (2018).

3 Der neue Regelungsrahmen der DS-GVO

Ab dem 25. Mai 2018 tritt nach einer zweijährigen Übergangsfrist die europäische Datenschutz-Grundverordnung (DS-GVO) in Kraft, die das Datenschutzrecht in Europa erstmals vereinheitlicht und für alle Mitgliedstaaten bindend sein wird. Über diverse Öffnungsklauseln wurden den nationalen Gesetzgebern jedoch Gestaltungsspielräume eingeräumt – zu viele, wie manche Autoren meinen.[1] Zusammen mit der Vielzahl der in der Verordnung ebenfalls enthaltenen unbestimmten Rechtsbegriffe dürfte dies wohl kaum – so die Befürchtung – zu einer einheitlichen Rechtslage beitragen.[2] Insbesondere der deutsche Gesetzgeber hat von den Öffnungsklauseln rege Gebrauch gemacht: Die novellierte Fassung des Bundesdatenschutzgesetzes (BDSG-neu) ergänzt, konkretisiert und modifiziert die DS-GVO in diversen Themenbereichen, u. a. indem etwa die Auskunftsrechte für Betroffene bei der Verarbeitung ihrer Daten zu statistischen Zwecken oder wissenschaftlichen Forschungszwecken eingeschränkt werden (§27 Abs. 2 BDSG-neu) bzw. datenverarbeitenden Stellen die Weiterverarbeitung/Sekundärnutzung von Daten zum Zwecke der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erlaubt wird (z. B. zur Fraud Prevention and Detection, siehe §24 Abs. 1 Nr. 2 BDSG-neu).

Die DS-GVO ist immer dann anzuwenden (sachlicher Anwendungsbereich), wenn personenbezogene Daten verarbeitet werden, mit der Ausnahme der Datenverarbeitung von natürlichen Personen im Rahmen persönlicher und familiärer Zwecke (sog. „Haushaltsausnahme“ wie das Führen eines privaten Telefonbuchs etc., siehe Art. 2 Abs. 2 lit. c DS-GVO). Die DS-GVO ist immer auch dann anzuwenden (räumlicher Anwendungsbereich), wenn personenbezogene Daten von Personen verarbeitet werden, die sich innerhalb der EU aufhalten (sog. Marktortprinzip nach Art. 3 Abs. 2 DS-GVO). Maßgeblich ist damit nicht mehr nur der Ort, an dem die datenverarbeitende Stelle ihren Sitz bzw. Niederlassung hat (und dem dortigen nationalen Datenschutzrecht – sofern vorhanden), sondern die Betroffenheit der sich in der EU befindlichen Personen durch die Datenverarbeitung. Das Marktortprinzip betrifft sowohl Unternehmen, die a) Waren und Dienstleistungen – entgeltlich oder unentgeltlich – innerhalb der Union anbieten (Art. 3 Abs. 2 lit. a DS-GVO) als auch b) Unternehmen, die das Verhalten von Personen in der EU lediglich beobachten (Art. 3 Abs. 2 lit. b DS-GVO). Der Gesetzgeber hat insbesondere mit der letzteren Formulierung der steigenden Bedeutung des Webtracking / von On- und Offline-Tracking im Rahmen von Big Data Rechnung getragen und ein höheres Schutzniveau für Verbraucher geschaffen.

Insgesamt trägt die DS-GVO deutlich die Handschrift der Lissaboner Verträge, die insgesamt auf eine Verschlankung des Staates und Privatisierung hoheitlicher Aufgaben abzielen.[3] Grundlegend neu ist in der DS-GVO der Wegfall der Meldepflicht der Datenverarbeitung bei den Aufsichtsbehörden und die Einführung einer Beweislastumkehr: Datenverarbeitende Stellen müssen nun jederzeit nachweisen können, dass die Datenverarbeitung im Einklang mit der Verordnung erfolgt (Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO und Art. 24 Abs. 1 DS-GVO). In bestimmten Einzelfällen sind jedoch vor Aufnahme der Datenverarbeitung die Aufsichtsbehörden zu konsultieren (Art. 36 DS-GVO). Die Rechenschaftspflicht geht einher mit umfangreichen Dokumentationspflichten wie dem Führen eines Verarbeitungsverzeichnisses (Art. 30 DS-GVO), wobei für Unternehmen mit weniger als 250 Beschäftigten Entlastungen vorgesehen wurden, sofern die Datenverarbeitung kein Risiko für die Rechte und Freiheiten der betroffe-

[1] Vgl. Roßnagel et al. (2016), S. XVII bzw. S. 180ff.
[2] Vgl. Roßnagel et al. (2016), S. XVII bzw. S. 180ff.
[3] Vgl. Lachaud (2016), S. 820.

nen Personen birgt (Art. 30 Abs. 5). Eine Vielzahl weiterer Neuregelungen, wie etwa das sog. Privacy-by-Design (Art. 25 Abs. 1) oder die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung bei hohen Risiken für die Rechte und Freiheiten der durch die Datenverarbeitung betroffenen Personen (Art. 35 DS-GVO) enthalten implizite Hinweise, dass mit der DS-GVO ein umfassendes betriebliches Frühwarn-, (Risiko-)Management- und Compliance-System erforderlich wird. Die DS-GVO unterlässt es aber (aufgrund der Unternehmensgröße und Branchenabhängigkeit?), dieses Management-System eingehender zu umreißen. In diesem Zusammenhang ist es wichtig zu erwähnen, dass das deutsche Modell des betrieblichen Datenschutzbeauftragten mit der DS-GVO nun europaweit für bestimmte Fälle der Datenverarbeitung zur Pflicht wird (Art. 37 DS-GVO). Im Sinne der Verträge von Lissabon enthält die DS-GVO aber auch neue Elemente zur Ko-Regulierung, einer „regulierten Selbstregulierung" für datenverarbeitende Branchen. Die schon in der Datenschutzrichtlinie enthaltene aber bisher wenig genutzte Möglichkeit zur Etablierung branchenspezifischer Verhaltenskodizes (Codes of Conduct) durch Branchenverbände wurde in die DS-GVO übernommen.[4] Codes of Conduct müssen jedoch nun von den Aufsichtsbehörden genehmigt werden (Art. 40 Abs. 5 DS-GVO). Zudem müssen Verfahren vorgesehen werden, die den Branchenverbänden die Überwachung der Einhaltung der Verhaltensregeln ermöglichen (Art. 40 Abs. 4 DS-GVO). Völlig neu hinzugekommen ist mit der DS-GVO die Möglichkeit zur Zertifizierung/Auditierung bzw. der Schaffung von Datenschutzsiegeln und -prüfzeichen (Art. 42 DS-GVO). Gemäß Art. 43 Abs. 2 lit. c DS-GVO sind hier ebenfalls Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzzertifizierung durch Zertifizierungsstellen festzulegen bzw. gemäß Art. 43 Abs. 2 lit. d DS-GVO Strukturen und Verfahren zu etablieren, mit denen bei Zertifizierungsstellen in öffentlich transparenter Weise Beschwerden eingereicht werden können und diesen nachgegangen wird.

Sehr vorteilhaft im Sinne einer verbesserten Durchsetzung des Datenschutzrechts ist die drastische Erhöhung des Sanktionsrahmens: Art. 83 Abs. 5 DS-GVO sieht Geldbußen von bis zu 20 Millionen Euro oder im Fall von Unternehmensgruppen von bis zu 4% des gesamten weltweit erzielten Jahresumsatzes vor. Auch sieht Art. 58 Abs. 1 lit. f DS-GVO nun erstmals die Möglichkeit einer datenschutzrechtlichen Hausdurchsuchung vor. Neben diesen erweiterten Befugnissen werden den Aufsichtsbehörden aber auch erweiterte Aufgaben zuteil: Neben die Hauptaufgabe der Überwachung und Durchsetzung (Art. 57 Abs. 1 lit. a DS-GVO) treten u. a. hinzu a) die Aufklärung/Sensibilisierung der Öffentlichkeit bzgl. Themen des Datenschutzes (Art. 57 Abs. 1 lit. b DS-GVO) und b) die Aufklärung von Unternehmen bzgl. ihrer Pflichten (Art. 57 Abs. 1 lit. d DS-GVO). Während gerade der Aufklärungsauftrag gegenüber Unternehmen als sehr begrüßenswert einzustufen ist, gibt es hierzu auch kritische Stimmen:[5] Es wird befürchtet, dass die Aufklärungsaufgabe die Aufsichtsbehörden möglicherweise dahingehend beeinflussen könnte, dass bei festgestellten Verstößen zunächst „nur" eine Aufklärung stattfindet und Sanktionen bei einem Erstverstoß ausbleiben. Hierfür würde jedenfalls sprechen, dass ein betroffenes Unternehmen gegenüber einer Sanktion einwenden könnte, die Behörde habe nicht ausreichend aufgeklärt.

Art. 4 Nr. 7 DSGVO definiert den Verantwortlichen der Datenverarbeitung. Dem Verantwortlichen obliegt die Aufgabe sicherzustellen, dass die Vorgaben der DS-GVO im Rahmen der Datenverarbeitung eingehalten werden. Da bei heutigen Verarbeitungsprozessen oft mehrere Stellen die Abläufe steuern, baut die DS-GVO die „gemeinsame Verantwortlichkeit" weiter aus: Der neu geschaffene Art. 26 DS-GVO soll die Beteiligten dazu anhalten, ihre Pflichten klarer und transparenter zu verteilen, um eine organisierte Verantwortungslosigkeit entgegenzuwirken.[6]

Als eine zentrale Neuerung statuiert Art. 20 DS-GVO ein „Recht auf Datenübertragbarkeit": Jede natürliche Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen

[4] Vgl. de Hert/Papakonstantinou (2016), S. 192.
[5] Vgl. Haag (2016).
[6] Vgl. Albrecht/Jotzo (2017), S. 61.

bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, diese an einen anderen Verantwortlichen zu übertragen bzw. übertragen zu lassen. Als „überschießendes Wettbewerbsrecht“ verfolgt diese Regelung in erster Linie nicht-datenschutzrechtliche Ziele: Die Regelung soll Lock-In-Effekte aufbrechen und den Wettbewerb zwischen den Anbietern von sozialen Plattformen, Kommunikations- und Clouddiensten fördern.[7] Zugleich – und eher ungewollt? – könnte diese Regelung aber auch zur Entstehung neuer Big-Data-basierter Geschäftsmodelle beitragen, bei denen betroffene Personen von Datensammlern bzw. Unternehmen animiert werden, ihre Nutzungsdaten für weiterführenden Analysen entgeltlich/unentgeltlich gemäß Artikel 20 DS-GVO übertragen zu lassen bzw. in einem maschinenlesbaren Format zur Verfügung zu stellen (etwa für Scoringzwecke u. ä.).[8] Zudem könnte das Recht auf Datenübertragbarkeit einer Ökonomisierung der informationellen Selbstbestimmung weiter vorschubleisten, indem Nutzerinnen und Nutzer ihre heruntergeladenen Daten gewinnbringend an unterschiedliche Akteure verkaufen.

[7] Vgl. Albrecht/Jotza (2017), S. 87.
[8] Vgl. Stiftung Datenschutz (2018), S. 4.

4 Trends, Treiber, Determinanten, Wildcards

Eine Vielzahl der Anpassungen in der DS-GVO sind im Hinblick auf Big Data vorgenommen worden, auch wenn man den Begriff „Big Data“ sowohl im Gesetzestext der DS-GVO als auch den nicht rechtlich bindenden Vorüberlegungen bzw. Auslegungserläuterungen, den sog. Erwägungsgründen (EWG), vergeblich sucht. Die DS-GVO ist höherrangig an den Grundsatz des „Verbots mit Erlaubnisvorbehalt“ bzw. den Grundsatz der Zweckbindung gebunden, die in Artikel 8 Abs. 2 der Charta der Grundrechte der Europäischen Union (GRCh) formuliert wurden: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn es gibt hierfür eine gesetzliche Grundlage oder die betroffene Person hat in die Datenverarbeitung eingewilligt. Zudem dürfen Daten nur zu festgelegten Zwecken (und damit definierten Kontexten) verarbeitet werden.

4.1 Zweckbindung und Weiterverarbeitung

Der Zweck legitimiert die Verarbeitung von personenbezogenen Daten und ist damit Dreh- und Angelpunkt hinsichtlich der Bewertung der Erforderlichkeit, der Angemessenheit / des Umfangs und der Dauer der Datenverarbeitung.[1] Art. 5 DS-GVO „Grundsätze der Verarbeitung personenbezogener Daten“ konkretisiert den in Art. 8 Abs. 2 GRCh formulierten Zweckbindungsgrundsatz und erlaubt die Datenverarbeitung nur für „festgelegte, eindeutige und legitime Zwecke“. Eine Sekundärnutzung/Weiterverarbeitung einmal erfasster Daten – im Sinne von Big Data – ist damit jedoch nicht gänzlich ausgeschlossen: Eine Weiterverarbeitung ist zulässig, sofern a) die Person darin eingewilligt hat, b) eine Rechtsvorschrift der Union oder der Mitgliedsstaaten dies ausdrücklich erlaubt oder c) die Weiterverarbeitung mit dem Ursprungszweck vereinbar ist (Art. 6 Abs. 4 DS-GVO wobei die Sekundärnutzung von Daten ohne Einwilligung lediglich aufgrund der festgestellten Vereinbarkeit mit den Primärzwecken mit gewissen Informationspflichten gegenüber den Betroffenen verbunden ist, siehe Art. 13 Abs. 3 DS-GVO).[2] Eine Weiterverarbeitung für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gilt ferner nicht als unvereinbar mit den ursprünglichen Zwecken (wissenschaftliche Forschung und Statistik als sog. privilegierte Sekundärzwecke gemäß Art. 5 Abs. 1 lit. b DS-GVO).

Die wissenschaftliche Literatur ist sich uneins darüber, welche Folgen die obigen Ausformulierungen des Zweckbindungsgrundsatzes für die weitere gesellschaftliche Diffusion von Big Data haben werden. So gibt es Stimmen, die darauf hinweisen, dass die DS-GVO zu enge Grenzen für Big Data ziehen würde: Der Zweckbindungsgrundsatz und der Grundsatz der Erforderlichkeit und der Datenminimierung liegt grundsätzlich quer zur zentralen Big-Data-Idee, möglichst viele Daten auf Vorrat anzulegen (und nach Zweckerfüllung nicht zu löschen) bzw. möglichst viele heterogene Datenbestände aus unterschiedlichen Quellen zu fusionieren und auszuwerten.[3] Zusammen mit dem Grundsatz, dass Daten nur zu eindeutig festgelegten Zwecken transparent nach „Treu und Glauben“ verarbeitet werden dürfen, stellt dies eine wesentliche Hürde für den Big-Data-Einsatz dar, weshalb sich Unternehmen auch aufgrund des hohen

[1] Vgl. Frenzel Art. 5 Rn. 23 in Paal/Pauly (2017).
[2] Zur Problematik der Feststellung der Vereinbarkeit von Primär- und Sekundärzweck vgl. Roßnagel et al. (2016), S. 159; Culik/Döpke (2017), S. 229.
[3] Vgl. Zarsky (2017), S. 1005f.; Roßnagel (2013), S. 564ff.

Bußgeldrahmens von einer Investition in Big-Data-Analysen scheuen würden.[4] Mit Blick auf die historischen Erfahrungen weisen dagegen andere Autoren darauf hin, dass datenverarbeitende Stellen bisher immer genügend Kreativität an den Tag gelegt hätten, die Zwecke weit, aber dennoch legal zu definieren.[5]

Uneinigkeit herrscht in der Literatur ferner darüber, ob sich Unternehmen darauf berufen können, bei Makro-Level-Analysen eine privilegierte Weiterverarbeitung zu statistischen Zwecken vorzunehmen, weil die DS-GVO es letztendlich versäumt, den Begriff Statistik eindeutig zu definieren.[6] Das Gros der Autoren ist der Ansicht, dass mit Statistik lediglich amtliche Statistik gemeint ist – auch in Kontinuität der bisherigen Rechtsprechung.[7] Die DS-GVO führt in dem nicht rechtlich bindenden EWG 162 DS-GVO aber lediglich aus, dass statistische Ergebnisse „für verschiedene Zwecke" genutzt werden können – ohne die verarbeitende Stelle weiter zu konkretisieren und einzuschränken. Statistische Daten dürfen aber keine personenbezogenen Daten sein, sondern nur aggregierte Daten, die nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden (EWG 162 DS-GVO, Satz 4). Das darin zum Ausdruck gebrachte Statistikverständnis erweist sich bei genauerer Hinsicht jedoch als verkürzend: Statistik – sei es im Staatswesen oder in der Wirtschaft – dient immer der Schaffung von Planungsgrundlagen, die im weitesten Sinne für Maßnahme und Entscheidungen gegenüber Betroffenen verwendet werden – wenn auch langfristig und mittelbar (BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83, Rn. 123, Rn. 162). Statistik ist deshalb – so könnte man argumentieren – auch für Unternehmen erlaubt, weil es allenfalls graduelle Unterschiede zwischen einer unternehmerischen und einer amtlichen Statistik gibt.

Alles in allem ist die Regelung zur Privilegierung der Statistik bzw. wissenschaftlichen Forschung wohl als ein weiteres Einfallstor für die Aufweichung der Zweckbindung zu werten, denn hier gilt für Außenstehende das Erfordernis nachzuweisen, dass die Privilegierung nicht greift (und etwa Big-Data-basierte Markt- und Meinungsforschung keine wissenschaftliche Forschung ist).[8] Das gleiche gilt für die Abwägung darüber, wann eine Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar und kompatibel ist – eine Abwägung, die mit der DS-GVO komplett der datenverarbeitenden Stelle anheimgestellt wird.[9] Für ein Verbot der Weiterverarbeitung muss nun nachgewiesen werden, dass die Weiterverarbeitung mit dem Primärzweck nicht vereinbar ist (Umkehr der Darlegungslast und Aufweichung des Zweckbindungsgrundsatz, siehe Frenzel Art. 5 Rn. 30 in Paal/Pauly 2017).

Der deutsche Gesetzgeber gesteht den datenverarbeitenden Stellen im Rahmen der Weiterverarbeitung von Daten sogar noch weitere Spielräume zu: Die Sekundärnutzung ist grundsätzlich auch zulässig für die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche (§24 Abs. 1 Nr. 2 BDSG-neu in Kontinuität von §26 Abs. 6 Nr. 3 BDSG-alt). Es ist nicht absehbar, in welchem Umfang sich Unternehmen auf diesen sehr offenen, vagen Passus für ihre Big-Data-Analysen beziehen werden und welche Folgen dies für von der Datenverarbeitung Betroffene in-the-long-run haben könnte.

Auch ist unklar, welche Wirkungen das „Recht auf Datenübertragbarkeit" (Art. 20 DS-GVO) in-the-long-run für zukünftige Big-Data-Lösungen und die Mehrfachnutzung von Daten zu Zwecken, die nicht mit dem Primärzweck kompatibel sind, entfalten könnte. Zwar sinkt mit der Mitnahmemöglichkeit der eigenen Daten die Schwelle zum Wechsel digitaler Anbieter, zum anderen könnte dies jedoch auch zur

[4] Vgl. Zarsky (2017), S. 1006.
[5] Vgl. Simitis (1990), S. 485; Roßnagel et al. (2016), S. 160.
[6] Vgl. Zarsky (2017), S. 1007f.
[7] Vgl. Frenzel Art. 5 Rn. 32 in Paal/Pauly (2017); Roßnagel et al. (2016) S. 159; Culik/Döpke (2017), S. 230.
[8] Vgl. Frenzel Art. 5 Rn. 32/33 in Paal/Pauly (2017).
[9] Vgl. Roßnagel et al. (2016), S. 159f.

Etablierung neuer Geschäftsmodelle beitragen, etwa in dem Unternehmen (Scoring-Dienstleister, Versicherungen, Werbeunternehmen etc.) Personen dazu animieren, ihre Daten mithilfe von Art. 20 DS-GVO an sie zu übertragen.[10] Im Sinne der Datensparsamkeit ist zudem anzumerken, dass die Datenübertragung nicht automatisch mit der Löschung des Ursprungsdatensatzes einhergeht und damit u. U. zu einer schwer kontrollierbaren Vielzahl an nichtsynchronisierten Duplikaten bei unterschiedlichen Akteuren führen kann.[11]

4.2 Rechtmäßigkeit der Verarbeitung: Einwilligung – vertragliche Erforderlichkeit – berechtigte Interessen – Kopplungsverbot

Der Zweckbindungsgrundsatz ist elementar für das europäische Datenschutzrecht. Zwecke müssen zum einen „festgelegt" und „eindeutig" sein (womit Blankettformeln ausgeschlossen sind, nicht jedoch unbestimmte, aber bestimmbare Begriffe innerhalb einer Zweckbestimmung mit einer hinreichenden Quantität und Qualität).[12] Zwecke müssen ferner auch „legitim" sein. Ein Zweck ist gemäß dem Prinzip des „Verbots mit Erlaubnisvorbehalt" dann legitim, wenn a) die betroffene Person den Verantwortlichen durch Einwilligung ermächtigt hat, die sie betreffenden personenbezogenen Daten zu verarbeiten oder b) eine gesetzliche Grundlage die Verarbeitung der personenbezogenen Daten ausdrücklich erlaubt. Art. 6 DS-GVO nennt hier als gesetzliche Erlaubnistatbestände u. a. eine Datenverarbeitung, die zur Erfüllung eines Vertrags oder einer vorvertraglichen Maßnahme erforderlich ist (Art. 6 Abs. 1 lit. b DS-GVO) bzw. eine Datenverarbeitung, die der Wahrung berechtigter Interessen der datenverarbeitenden Stelle dient (Art. 6 Abs. 1 lit. f DS-GVO). Mit Frenzel kann festgestellt werden, dass die Bezeichnung „Verbotsprinzip" insgesamt mehr verspricht, als dass das fein ausdifferenzierte System der Erlaubnistatbestände in Art. 6 DS-GVO tatsächlich hält.[13]

Als eine wesentliche Neuerung wurde mit der DS-GVO das sog. „Kopplungsverbot" eingeführt (Art. 7 Abs. 4 DS-GVO). Als überschießendes Verbraucherschutzrecht soll es verhindern, dass von einer Datenverarbeitung Betroffene dazu genötigt werden, in eine Preisgabe von Daten einzuwilligen, die für die Erfüllung eines Vertrags (für die Erbringung einer Dienstleistung bzw. eines Online-Dienstes) nicht erforderlich ist. In einer sehr strikten Lesart des Kopplungsverbots sehen einige Autoren das Ende der Big-Data-basierten Silicon-Valley-Geschäftsmodelle heraufdämmern, bei denen Nutzerinnen und Nutzer mit ihren Daten für die erbrachten Dienste bezahlen. So ist etwa Albrecht/Jotzo der Ansicht, dass z. B. für die Bereitstellung von Kommunikationsmöglichkeiten über ein soziales Netzwerk („zu erbringender Dienst") die umfassende werbetechnische Analyse als auch Weitergabe von Daten nicht unbedingt erforderlich ist (weshalb – gemäß einer strikten Auslegung des Kopplungsverbots – eine Einwilligung der Nutzer darin auch unwirksam wäre).[14] Das Gros der Autoren äußerst sich hier jedoch zurückhaltender und verweist auf die zentrale Umgehungsmöglichkeit, die werbetechnische Datenverarbeitung als Entgelt selbst zum Vertragsgegenstand zu erheben, mithin die Datenverarbeitung der Big-Data-basierten Silicon-Valley-Geschäftsmodelle „Daten als Entgelt" komplett auf Art. 6 Abs. 1 lit. b DS-GVO zu stützen.[15] Bzgl. der Auslegung des Kopplungsverbots ist jedoch noch vieles im Unklaren, und die öffentlichen Diskussionen über die gesellschaftlichen Chancen und Risiken dieser Silicon-Valley-Geschäftsmodelle,

[10] Vgl. Stiftung Datenschutz (2018) S. 3f.
[11] Vgl. Stiftung Datenschutz (2018). S. 3f.
[12] Vgl. Frenzel Art. 5 Rn. 27 in Paal/Pauly (2017).
[13] Vgl. Frenzel Art. 6 Rn. 1 in Paal/Pauly (2017).
[14] Vgl. Albrecht/Jotzo (2017), S. 71f.
[15] Vgl. Frenzel Art. 7 Rn. 18ff. in Paal/Pauly (2017); Engeler (2018).

die mit der Verarbeitung einer Vielzahl intimer und sensibler Daten einhergeht, haben angesichts der jüngsten Skandale um Facebook und Cambridge Analytica bzw. den Enthüllung von Edward Snowden erst begonnen. Inwiefern das Kopplungsverbot insgesamt die Schaffung alternativer datenschutzfreundlicher Bezahldienste fördert, die nicht Daten als Entgelt verwenden, ist zum jetzigen Zeitpunkt unklar.[16]

Das Kopplungsverbot ist wohl auch in anderen Verarbeitungsfällen nur eingeschränkt gültig: Für Online-Händler ist der Versand von personalisierter Werbung höchstwahrscheinlich auch über Erlaubnistatbestand Art. 6 Abs. 1 lit. f DS-GVO „berechtigtes Interesse" legitimierbar. Zumindest erwähnt EWG 47 den Terminus „Direktwerbung" als einen möglichen legitimen Zweck im Rahmen der vorzunehmenden Interessenabwägung.[17] Das berechtigte Interesse „Direktwerbung" erlaubt jedoch nicht per se die Erstellung von Persönlichkeitsprofilen und die Verarbeitung besonderer Kategorien personenbezogener Daten (siehe hierzu Abschnitt 4.3 und 4.5) – beides Strategien, die ein One-to-one-Marketing oft erheblich effektiver gestalten würden.

4.3 Profiling, Scoring, automatisierte Entscheidungen und entscheidungsunterstützende Systeme

Eine wesentliche Anwendung von Big Data auf Mikroebene ist das Profiling und Scoring natürlicher Personen. Während man den Begriff „Big Data" in der DS-GVO vergeblich sucht, definiert Art. 4 Nr. 4 DS-GVO Profiling als jedwede „[…] Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen". Der Gesetzgeber reagiert mit der Aufnahme des Begriffs „Profiling" in die DS-GVO auf die Tatsache, dass moderne (Big-Data-basierte) Datenanalyseanwendungen / Data-Mining-Verfahren immer häufiger dazu eingesetzt werden, um Aussagen über die Eigenschaften von Menschen und ihrem künftigen Verhalten zu treffen.[18] Da sich diese Entwicklungen angeblich noch in einem frühen Stadium befinden, hat der Gesetzgeber – auch im Sinne einer gewissen Innovationsoffenheit – auf eine eigenständige, restriktive Rechtsgrundlage für Profiling verzichtet und dieses pauschal den sog. automatisierten Einzelentscheidungen nach Art. 22 DS-GVO zugeordnet.[19] Art. 22 Abs. 1 DS-GVO – in Kontinuität von Art. 15 DS-RL – statuiert das Recht, dass niemand einer Entscheidung unterworfen wird, die rechtliche und andere erhebliche Folgen für ihn hat und ausschließlich auf einer automatisierten Verarbeitung beruht – es sei denn die Verarbeitung ist vertraglich erforderlich, beruht auf einer Rechtsnorm der Union / eines Mitgliedsstaates oder die Person hat darin freiwillig und informiert eingewilligt (Art. 22 Abs. 2 DS-GVO). Art. 22 Abs. 3 nennt für Fälle einer automatisierten Entscheidung ferner für Betroffene das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Anfechtung der Entscheidung durch den Betroffenen und Darlegung des eigenen Standpunktes. Art. 15 Abs. 1 lit. h gesteht den Betroffenen zudem im Falle automatisierter Entscheidungen erweiterte Informationsrechte zu: Die datenverarbeitende Stelle hat bei automatisierten Entscheidungen „[…] aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen" bereitzustellen. Im Fall von Profiling / automatisierten Entscheidungen hat der Verantwortliche der Datenverarbeitung auf jeden Fall

[16] Zur Hoffnung, dass das Kopplungsverbot die Verbreitung von Bezahl-Diensten fördern würde vgl. Albrecht/Jotzo (2017), S. 72.
[17] Vgl. Specht (2017), S. 1041.
[18] Vgl. Albrecht/Jotzo (2017), S. 60; S. 78f.
[19] Vgl. Albrecht/Jotzo (2017). S. 60; S. 78f.; Martini Art. 22 Rn. 8 in Paal/Pauly (2017).

eine Datenschutz-Folgeabschätzung gemäß Art. 35 DS-GVO vorzunehmen (Art. 35 Abs. 3 lit. a DS-GVO).

Auffallend ist insgesamt, dass Profiling nur als „automatisiertes" Verarbeitungsverfahren in den Blick gerät, Art. 22 DS-GVO mit den erweiterten Rechenschafts- und Auskunftsrechten nur dann greift, wenn es sich um Verfahren handelt, die „ausschließlich" auf automatisierten Entscheidungen basieren. Das Europäische Parlament hatte in einem frühen Gesetzesentwurf hier noch die Formulierung „vorwiegend" vorgesehen, die jedoch in der endgültigen Fassung gestrichen wurde.[20] Die Formulierung „ausschließlich" schafft jedoch ein Schlupfloch bzw. Regelungslücke, da durch die (pro forma) Hinzunahme eines menschlichen Entscheiders Art. 22 (und die damit verbundenen, erweiterten Rechenschaftspflichten) einfach umgangen werden könnte.[21] Der Gesetzgeber hat es damit versäumt, die Vielzahl der auf Big Data, Profiling und Scoring basierenden Entscheidungsunterstützungssysteme zu regulieren, insbesondere im Hinblick auf ihre potentiell diskriminierenden Effekte für Betroffene und die Erkennung dieser Effekte durch Betroffene.

Auch ist unklar, inwiefern in Zeiten neuronaler Netze und Deep Learning überhaupt aussagekräftige Informationen über das Zustandekommen automatisierter Entscheidungen geliefert werden können, sind derartige Systeme doch oft eine Black Box.[22] Als Black Box können die Auskunftsansprüche und ein Recht auf Erklärung bei automatisierten Entscheidungen aber kaum wirkungsvoll umgesetzt werden, weshalb u. a. in den USA das Kredit-Scoring auf Basis maschinellen Lernens verboten ist.[23] Die DS-GVO selbst kennt überhaupt keine Spezialregelungen zu Scoring.[24] In §31 Abs. 1 BDSG-neu (in Kontinuität von §28b BDSG-alt) finden sich lediglich Spezialregelung für das Scoring im Rahmen der Bonitätsbewertung: Das BDSG verbietet das Scoring zum Zwecke der Ermittlung der Bonität a) nur auf Basis von Anschriftendaten (indem etwa ein Bonitätsmittelwert der umliegenden Anrainer gebildet wird) bzw. b) nennt das Erfordernis, dass für die Ermittlung des Scores ein „wissenschaftlich anerkanntes mathematisch-statistisches Verfahren" verwendet werden muss und c) die verwendeten Daten des Scores „erheblich" mit den zu bewertenden Aspekten zusammenhängen. Ob neuronale Netze als mathematisch-statistische Verfahren betrachtet werden können, weil sie ja statistisch-induktiv lernen, ist aufgrund der Offenheit der Formulierung unklar. Die Formulierung des BDSG, dass nur „wissenschaftlich anerkannte mathematisch-statistische Verfahren" für ein Scoring verwendet werden dürfen, hat sich in der Praxis für Aufsichtsbehörden als schwierig überprüfbar herausgestellt – mit unklaren Effekten für Betroffene und die Gesellschaft als Ganzes: Die Prüfung der Zulässigkeit der Scoring-Verfahren scheitert damit meist im Ansatz, bevor die Erheblichkeit der verwendeten Daten bestimmt werden kann.[25] Unklar ist auch, wie Gerichte die Einschaltung von Alibi-Entscheidern in Entscheidungsprozesse zukünftig bewerten werden: Es kann gut sein, dass auch entscheidungsunterstützende Systeme, die die Entscheidung des Menschen maßgeblich vorbereiten, als automatisierte Entscheidungen eingestuft werden, sofern nicht der Nachweis erbracht werden kann, dass der Entscheider von seiner Entscheidungsmacht auch tatsächlich Gebrauch gemacht hat.[26]

Da sich bisher nur sehr vage abzeichnet, welche tatsächlichen Chancen und Risiken Big-Data-basierte Anwendungen insbesondere im Bereich Profiling / Scoring / automatisierte Einzelfallentscheidungen haben, soll der Europäische Datenschutzausschuss zukünftig das Thema mit Leitlinien begleiten (Art. 70

[20] Vgl. Wachter et al. (2017), S. 96.
[21] Vgl. Wachter et al. (2017), S. 88; Zarsky (2017), S. 1016.
[22] Vgl. Kuner et al. (2017).
[23] Vgl. Mittelstadt et al. (2016) S. 14.
[24] Vgl. Moos/Rothkegel (2016), S. 567.
[25] Vgl. ULD / GP Forschungsgruppe (2014), S. 174; Weichert (2014), S. 170.
[26] Vgl. Zarsky (2017), S. 1016; Martini Art. 22 Rn. 16ff. in Paal/Pauly (2017).

Abs. 1 lit. f. DS-GVO).[27] Art. 22 DS-GVO entspricht in seinem Wesensgehalt Art. 15 DS-RL (Verbot mit Erlaubnisvorbehalt). Das Hinzufügen des Begriffs „Profiling“ in Art. 22 DS-GVO bringt keine wesentliche Veränderung, sondern wird wohl primär Anknüpfungspunkt sein für die anstehenden wichtigen gesellschaftlichen Debatten zum Thema.[28]

4.4 Verarbeitung personenbezogener Daten und anonymer Daten

Für Big-Data-Analysen auf dem Mikrolevel – etwa bei der Online-Werbung, dem Behavioural Targeting und Retargeting – ist es oft gar nicht interessant zu wissen, welchen Namen eine Person hat bzw. welche reale Person sich dahinter verbirgt: Es genügt für die Anwendungszwecke, eine Person durch andere Merkmale zu individualisieren und kategorisieren, um Systemanpassungen auszulösen.[29] Die Grenzen zwischen legitimer Differenzierung und illegitimer Diskriminierung sind dabei oft fließend wie das Beispiel der Online-Preisdifferenzierung nach Personenkategorien zeigt.[30] Insbesondere die Werbeindustrie ist der Ansicht, dass sie überhaupt keine personenbezogenen Daten verarbeiten würde, wodurch das Datenschutzrecht überhaupt nicht mehr einschlägig wäre.[31] Es wird der Standpunkt vertreten: We „serve ads to you based on your identity […]. But that doesn't mean you're identifiable”.[32] Und: „The beauty of what we do is we don't know who you are […]. We don't want to know anybody’s name. […] All we want to do is […] have these attributes associated with them”.[33]

Während das herrschende EU-Datenschutzregime für das Cookie-Tracking z. B. eine Einwilligung des Nutzers erfordert, ist dies für das Auslesen von Betriebssystem- und Browserinformationen nicht der Fall. Diese Informationen werden in einem rechtlichen Graubereich zur Zeit oft als „nicht-personenbezogene Daten“ interpretiert, womit sie eine Basis dafür abgeben, iPhone-Nutzern etwa einen höheren Preis in Online-Shops anzuzeigen als anderen.[34] Um aber das Anti-Diskriminierungsrecht mit dem Datenschutzrecht zu verschränken, plädieren einige Autoren nachdrücklich dafür, auch dann anonyme Daten konsequent als personenbezogene Daten zu interpretieren, wenn sie eine selektive Wirkung entfalten und erhebliche Effekte für das Subjekt zeitigen, denn das Schutzziel des Datenschutzrechts ist ja gerade, dass eine betroffene Person frei entscheiden können soll, wer was über sie/ihn weiß, um sich vor negativen Folgen schützen zu können.[35] Ob letztere Kategorie von Daten als personenbezogene Daten interpretiert wird, hängt wesentlich davon ab, wie die demnächst zu verabschiedende ePrivacy-Verordnung (ePV) aussehen wird. Insbesondere die Digitalwirtschaft sieht sich durch den vorliegenden Entwurf massiv in ihren Interessen bedroht: Sämtliche Tracking-Mechanismen, sowohl online als auch offline, werden

[27] Vgl. Albrecht/Jotzo (2017), S. 60.
[28] Vgl. Albrecht/Jotzo (2017), S. 60.
[29] Vgl. Roßnagel (2013), S. 562.
[30] Vgl. Borgesius/Joost (2017).
[31] Vgl. Borgesius (2016), S. 256; Barocas/Nissenbaum (2014), S. 54. Dies wurde auch jüngst wieder ersichtlich bei den Kontroversen um den Einsatz von Gesichtsscannern in Real-Supermärkten zur Anzeige individualisierter Werbung.
[32] Industriestatement zitiert nach Barocas/Nissenbaum (2014), S. 54.
[33] Industriestatements zitiert nach Barocas/Nissenbaum (2014), S. 54.
[34] Vgl. Borgesius/Joost (2017), S. 358. Die Autoren weisen aber auch darauf hin, dass die rechtlichen Hürden für eine individualisierte Bepreisung im Rahmen der DS-GVO recht hoch sein dürften: Zum einen sind die Nutzerinnen und Nutzer im Rahmen der Datenschutzerklärung über die gesammelten Datenkategorien und Verarbeitungszwecke dezidiert aufzuklären. Zum anderen stellt die individualisierte Bepreisung eine Form der automatisierten Entscheidung nach Art. 22 DS-GVO dar, die grundsätzlich zustimmungspflichtig ist und für die verschärfte Informations- und Verarbeitungserfordernisse gelten.
[35] Vgl. Borgesius (2016).

technologieneutral als einwilligungsbedürftig kategorisiert. Die Nutzung von Rechen- und Speicherfähigkeit von Endgeräten sowie das Erheben jeglicher Informationen (Gerätekennungen einschließlich Informationen über die Beschaffenheit von Hard- oder Software) sind zunächst verboten (Art. 8 ePV, Entwurf vom 10.01.2017).

In der Bestimmung, was personenbezogene Daten und was anonyme Daten sind, geht die DS-GVO insgesamt einen pragmatischen Mittelweg zwischen den Ansätzen des „absoluten Personenbezugs“ und des „relativen Personenbezugs“: Sie begrenzt die zu berücksichtigenden Mittel auf die Mittel, die „angemessen“ sind und vom Verantwortlichen oder einem Dritten „wahrscheinlich genutzt“ werden.[36] Die Bewertung muss einzelfallspezifisch erfolgen und umfasst Faktoren wie Kosten der Identifizierung, Zeitaufwand, zum Zeitpunkt der Verarbeitung verfügbare Technologien etc. (EWG 26 DS-GVO).[37]

Dennoch ist die Strategie der Umgehung des Datenschutzrechts qua Verarbeitung lediglich anonymer Daten bei Big Data oft mit einem grundlegenden Problem behaftet: Die anonymen Spuren in ihrer Kombination sind oft zu genau und individuell, als dass eine De-Anonymisierung nicht mit vertretbaren Aufwand und denkbar anwendbaren Mitteln möglich wäre.[38] Viele für Big-Data-Analysen verwendete Daten sind deshalb – auch wenn angeblich anonym – wohl als personenbezogene Daten einzustufen.[39] Technische Ansätze der „Differential Privacy“ versuchen zwar, die anonymisierten Daten mit einem Rauschen zu versehen, um eindeutige Zuordnungen unmöglich zu machen. Inwiefern dieser Ansatz jedoch insgesamt erfolgsversprechend ist, bleibt unklar. Denn: Wo das Rauschen hinzugefügt wurde, darf im Sinne des Verhinderns einer De-Anonymisierung den Daten ja nicht ersichtlich sein. Zugleich wird mit dem Einführen eines Rauschens jedoch die Datenqualität verändert, was wiederum Einfluss auf die Güte, Zuverlässigkeit und Erklärungswert der Big-Data-Analysen insgesamt hat. Inwiefern also das Anonymisierungs-Paradoxon von Big Data mit technischen Lösungsansätzen wirklich aufgelöst werden kann – oder doch eben ein Paradoxon bleiben muss, das es anzuerkennen gilt –, ist offen und bedarf der weiteren kontextspezifischen Begleitforschung.

4.5 Verarbeitung besonderer Kategorien personenbezogener Daten

Die DS-GVO untersagt in Art. 9 Abs. 1 die Verarbeitung von Daten, „[…] aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“. Die Liste ist nahezu deckungsgleich mit den in Art. 21 Abs. 1 GrCh genannten Kategorien des Verbots der Diskriminierung. Die Grundrechtecharta nennt in einer nicht-abschließenden Aufzählung exemplarisch jedoch noch weitere Kategorien, die die DS-GVO nicht nennt: Das Verbot der Diskriminierung aufgrund „der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters“. Spiros Simitis, einer der Urväter des deutschen Datenschutzrechts, hat bereits in den 1990er Jahren in seinem Artikel „Sensitive Daten – Zur Geschichte und Wirkung einer Fiktion“ detailliert ausgeführt, wie hoffnungslos das

[36] Vgl. Albrecht/Jotzo (2017), S. 58f.
[37] Vgl. Albrecht/Jotzo (2017), S. 59. EWG 26 stellt auch klar, dass im Fall der sog. Pseudonymisierung personenbezogener Daten (im Sinne von Art. 4 Nr. 5 DS-GVO) immer das Datenschutzrecht einschlägig ist, weil der Verantwortliche typischerweise über die notwendigen Informationen (Schlüssel) verfügt, um die Daten zu reindividualisieren.
[38] Vgl. Roßnagel (2013), S. 565.
[39] Vgl. Roßnagel (2013), S. 563.

Unterfangen ist, eine allgemeingültige Liste von besonders schützenswerten Datenkategorien aufzustellen.[40] Die Sensitivität bemisst sich vielmehr nach dem Verarbeitungszweck und dem Verarbeitungskontext.[41] Ob also beispielsweise eine Angabe zur Gewerkschaftszugehörigkeit sensitiv ist (und potentiell diskriminierende Effekte gegenüber einem Individuum entfalten kann), ist je nach Land, Unternehmen etc. unterschiedlich, ebenso wie u. U. die Bedeutung des Besitzes eines iPhones. Das Bundesverfassungsgericht hat diesem Sachverhalt in seinem berühmten Volkszählungsurteil Rechnung getragen, indem es festgestellt hat, dass es in Zeiten der automatischen Datenverarbeitung „kein belangloses Datum mehr gibt" (BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83, Rn. 176). Die neuen Möglichkeiten, menschliche Gefühle, Gedanken, Absichten, Neigungen und Aversionen zu erfassen und zu verarbeiten, eröffnen ein weiteres Feld höchster Sensitivität, das in den Kernbereich der persönlichen Lebensführung eingreift und doch nicht vom bestehenden datenschutzrechtlichen Regelungskonzept der besonderen Kategorien personenbezogener Daten umfasst wird.[42] Ohnehin ist es eine Grundfigur des Datenschutzrechtes seit seinen Anfängen, zwar der „Sensitivität" von Daten Rechnung zu tragen, sie aber mit einer Vielzahl von Ausnahmen zu versehen, die auf eine weitgehende Freigabe der Verarbeitung hinauslaufen.[43] Auch die DS-GVO erlaubt die Verarbeitung besonderer Kategorien personenbezogener Daten, wenn u. a. die betroffene Person darin eingewilligt hat (Art. 9 Abs. 2 lit. a DS-GVO). Es ist unklar und bedarf der weiteren Forschung genau zu erörtern, inwiefern Big Data neue Diskriminierungspotentiale bietet und spezifische soziale Gruppen in der Chancengleichheit und gesellschaftlichen Teilhabe eingeschränkt werden.

4.6 Vertragsfreiheit – Einwilligung – Transparenz der Datenverarbeitung

Die Verarbeitung sensitiver Daten ist nach DS-GVO ebenso verboten wie der Einsatz automatisierter Entscheidungsverfahren oder etwa die Weiterverarbeitung von Daten zu anderen Zwecken – es sei denn, die Person hat darin eingewilligt. Die Einwilligung stellt damit – abgesehen von speziellen Erlaubnistatbeständen (vertragliche Erforderlichkeit der Datenverarbeitung, berechtigte Interessen, privilegierte Sekundärzwecke etc.) – eine der zentralen rechtlichen Grundlagen für Big-Data-Analysen dar. Die DS-GVO definiert Einwilligung als eine „[…] in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist." (Art. 4 Nr. 11 DS-GVO). Insbesondere die neue Formulierung „eindeutig bestätigende Handlung" schließt konkludente Zustimmungen in Zukunft wohl aus.[44] Ferner muss das Ersuchen um Einwilligung in „verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erfolgen (Art. 7 Abs. 2 DS-GVO). Neu hinzugekommen ist in der DS-GVO insgesamt die sog. Transparenzpflicht: Daten müssen in einer für die Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO) – wobei es hierfür egal ist, über welche Rechtgrundlage die Verarbeitung legitimiert wurde (Einwilligung, vertragliche Erforderlichkeit etc.). Art. 12 Abs. 7 DS-GVO führt dazu weiter aus, dass die zu gebenden Informationen in Kombination mit standardisierten Bildsymbolen bereitgestellt werden können (nicht müssen), „um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermit-

[40] Vgl. Simitis (1990).
[41] Vgl. Simitis (1990), S. 473.
[42] Vgl. Weichert (2017), S. 543. In der Literatur werden derartige Analysen v. a. unter dem Stichwort des „Big-Five-Modells" bzw. „OCEAN-Modells" diskutiert.
[43] Vgl. Simitis (1990), S. 476.
[44] Vgl. de Hert/Papakonstantinou (2016), S. 187.

teln“ (wobei die Symbole maschinenlesbar sein müssen und die Kommission es sich vorbehält, die Bildsymbole selbst zu standardisieren, siehe Art. 12 Abs. 7 Satz 2 und Art. 12 Abs. 8 DS-GVO). Auch das Bundesjustizministerium setzt sich im Sinne des Verbraucherschutzes für die Etablierung einer kompakten „Datenschutzerklärung auf einer Seite“ (sog. „One Pager“) ein und stellt dementsprechende Leitlinien zur Verfügung.[45] Rechtlich bindend ist der One-Pager und die Verwendung von Bildsymbolen jedoch nicht.

Während eine soziale Gruppe des Datenschutzdiskurses viel Arbeit darauf verwendet, die Informationslage in Form eines One-Pagers zu verbessern, steht dem eine andere Gruppe recht skeptisch gegenüber. Sie begrüßt zwar die Bemühungen, hält jedoch das damit verbundene Transparenz-Paradoxon der Datenverarbeitung für grundsätzlich nicht auflösbar: Selbst wenn die betroffenen Personen den in einfacher und klarer Sprache gehaltenen Text verstehen, können sie nicht informiert einwilligen bzw. informiert einen Vertrag eingehen, weil die Aggregation und Abstraktheit eben kein Verständnis bzw. keine Vorstellung darüber entstehen lässt, was wirklich „unter der Haube“ mit den Daten passiert – auch weil die Folgen von Big-Data-Analysen ex-ante kaum seriös abschätzbar sind.[46] Der gleiche Einwand gilt natürlich auch für maschinenlesbare Datenschutzerklärungen, mit denen Software-Agenten in entlastender Absicht für den Nutzer die Bedingungen der Datenverarbeitung aushandeln sollen. Derartige Lösungen erben zudem die klassischen Probleme im Hintergrund agierender autonomer Systeme: Transparenz, Nachvollziehbarkeit von Entscheidungen, Vertrauenswürdigkeit, Safety/Security, situationsadäquate Signalisierung und ggfs. Einbeziehung des Nutzers, Fehlfunktion, deren Erkennung und Haftung. Während also die eine Seite die Grenzen einer transparenten Datenverarbeitung betont und darauf aufmerksam macht, dass die vorgestellten Lösungen eher Scheinlösungen sind und mehr staatliche, bereichsspezifische Regulierung erforderlich ist bzw. eine Beschränkung der datenschutzrechtlichen Einwilligung angezeigt ist und eine bessere Kontrolle vertraglicher Klauseln durch Aufsichtsbehörden notwendig ist (auch um basale Verfassungswerte zu schützen), hält die andere Seite die oben genannten Lösungsansätze in pragmatischer Absicht für angemessene und zielführende Verbesserungen (wobei staatliche Regulierung oft als Paternalismus und unzulässige Bevormundung der betroffenen Personen dargestellt wird).[47]

4.7 Regulation und Selbstregulation

Das Aufgabenspektrum der Aufsichtsbehörden wurde mit der DS-GVO ausgeweitet: Neben die klassischen Aufgaben der Überwachung und Durchsetzung der Verordnung bzw. dem Nachgehen von Beschwerden treten nun u. a. auch umfassende Bildungs- und Aufklärungstätigkeiten gegenüber Öffentlichkeit und Unternehmen (siehe dazu im Einzelnen Art. 57 DS-GVO, der insgesamt 22 Aufgaben für die Aufsichtsbehörden nennt). Nur wenige Aufsichtsbehörden sehen sich jedoch personell, methodisch und technisch für diese Aufgaben gerüstet.[48] Insbesondere für technische Prüfungen von IT-Anwendungen und IT-Systemen im Sinne einer proaktiven Überwachung fehlt den Behörden die notwendige Ausstattung: Gerade einmal 10 Aufsichtsbehörden in der BRD verfügen über ein eigenes Prüf- oder IT-Labor,

[45] Vgl. BMJV (2015).
[46] Vgl. Barocas/Nissenbaum (2014), S. 58f.
[47] Für eine kritische Einschätzung der Wirksamkeit des One-Pager-Ansatzes vgl. Kettner et al. (2018). Für die Ausweitung der Zuständigkeiten der Datenschutzaufsichtsbehörde auf eine Klauselkontrolle vgl. Lewinski/Herrmann (2017b). Ein Beispiel für eine gesetzliche Festlegung/Einschränkung der Einwilligungsrahmenbedingungen ist in §26 Abs. 2 BDSG-neu zu finden: Von einer Freiwilligkeit der Einwilligung ist im Beschäftigtenverhältnis insbesondere dann auszugehen, „[…] wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen“.
[48] Vgl. Schulzki-Haddouti (2017), S. 120.

wobei keines der Labors über ein separates Budget verfügt.[49] Lediglich zwei Bundesländer weisen für das Prüf- und IT-Labor separates Personal aus in der Höhe von 0,5 Vollzeitäquivalenten.[50] Die DS-GVO sieht jedoch mit Art. 40 DS-GVO („Codes of Conduct") und Art. 42 DS-GVO („Audit und Zertifizierung") umfassende Elemente der Ko-Regulierung vor, die die Aufsichtsbehörden potentiell entlasten sollen. Beide Elemente, sowohl das Aufstellen von Verhaltensregeln als auch die Auditierung/Zertifizierung, sind jedoch gesetzlich nicht verpflichtend. Für Branchenverbände und Unternehmen könnte eine klare Anreizstruktur zur Umsetzung derartiger Maßnahmen fehlen, was sich an der bisherigen Erfolglosigkeit der Möglichkeit zur Aufstellung von Codes of Conduct im Rahmen der EU-Datenschutzrichtlinie gezeigt hat.[51]

Ein problematisches Element der Selbstregulation (im Sinne einer erweiterten Entscheidungsfreiheit für die datenverarbeitende Stelle) sind eventuell auch die Verfahrensweisen zur Meldung von Verletzungen des Schutzes personenbezogener Daten.[52] Nach Art. 31 Abs. 1 DS-GVO steht der datenverarbeitenden Stelle der Entscheidungsspielraum zu, selbst zu entscheiden, ob eine Datenpanne zu „Risiken von Rechten und Freiheiten einer betroffenen Person" geführt hat, was letztendlich den Effekt haben könnte, dass Datenpannen nicht an Aufsichtsbehörden gemeldet werden. Datenpannen, die nicht gemeldet werden, sind lediglich eigenverantwortlich zu dokumentieren (Art. 31 Abs. 5 DS-GVO). Auch sieht Art. 34 Abs. 3 DS-GVO Einschränkungen bei der Benachrichtigung von Betroffenen vor, deren Auswirkung ebenfalls schwer abzuschätzen sind. Art. 34 Abs. 3 lit. b sieht etwa eine Ausnahme von der Benachrichtigung der Betroffenen vor, wenn der „[…] Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht".

Im Sinn der Effektivierung des Datenschutzrechts und der Absenkung der Hemmschwelle zur Rechtsdurchsetzung führt die DS-GVO als eine wesentliche Innovation mit Art. 80 ein Verbandsklagerecht ein: Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht dürfen entweder im Auftrag einer betroffenen Person (Art. 80 Abs. 1 DS-GVO) oder selbst (Art. 80 Abs. 2 DS-GVO) bei Rechtsverstößen tätig werden – sofern dies im nationalen Recht vorgesehen ist. Die BRD verfügt mit dem „Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts" seit dem 23.02.2016 über eine derartige Klagebefugnis (BGBl. I v. 23.02.2016). Neben den klassischen Verbraucherschutzverbänden formieren sich mit der „Gesellschaft für Freiheitsrechte e. V." und „NOYB – European Center for Digital Rights" zunehmend auch neue Datenschutz-NGOs, die mit dem Instrument der strategischen Klage grundlegende Weichenstellungen im Sinne des Verbraucherschutzes bzw. des Schutzes basaler Verfassungswerten durchsetzen wollen. Ihnen ist jedoch eines mit den Aufsichtsbehörden gemein: Auch sie verfügen nur über sehr beschränkte finanzielle Mittel, was die Handlungsfähigkeit entsprechend einschränkt und eine Fokussierung erfordert.

[49] Vgl. Schulzki-Haddouti (2017), S. 122.
[50] Vgl. Schulzki-Haddouti (2017), S. 122.
[51] Vgl. Lachaud (2016), S. 825; de Hert/Papakonstantinou (2016), S. 192.
[52] Vgl. de Hert/Papakonstantinou (2016), S. 191.

5 Fazit und Ausblick

Mit der DS-GVO verfolgt der Gesetzgeber eine doppelte Zielrichtung: Zum einen soll der neue Rechtsrahmen effektiv die Grundrechte der Bürgerinnen und Bürger schützen, zum anderen aber auch die Wirtschaft und den digitalen Binnenmarkt fördern.[1] Die DS-GVO zielt zudem auf Bürokratieabbau durch Verlagerung einst hoheitlicher Aufgaben auf private Schultern und die Einführung von Instrumenten der Selbst- und Ko-Regulation. Selbst- und Ko-Regulation sind jedoch dann als unangemessene Regulierungsansätze anzusehen, wenn basale verfassungsrechtliche Grundwerte in einem schwerwiegenden Konflikt zueinanderstehen stehen bzw. Regelungsfelder betroffen sind, die politisch hinsichtlich der Regulierungsinhalte stark umstritten sind.[2] Beides dürfte für das Datenschutzrecht zu einem gewissen Grad zu bejahen sein. Wie angemessen und effektiv der neue Regulierungsrahmen der DS-GVO mit seinen Elementen der Selbst- und Ko-Regulation ist bzw. wie gut der Ausgleich zwischen Konsumentenschutz einerseits und Innovationsförderung andererseits gelungen ist, wird sich in den nächsten Jahren zeigen müssen.[3] Die DS-GVO führt zwar einige Elemente einer Ko-Regulation ein, belässt diese jedoch auf rein optionaler Basis. Eine Vielzahl zentraler Aspekte von Big-Data-Analytics bleibt deshalb – wohl auch im Sinne einer gewissen Innovationsoffenheit – unreguliert. Mit den „Guidelines on the protection of individuals with regard to processing of personal in the age of Big Data" formuliert der Europarat zwar zentrale Erfordernisse, wie ein verantwortungsvoller Einsatz von entscheidungsunterstützenden, Big-Data-basierten Expertensystemen aussehen könnten:[4]

„7.1 The use of Big Data should preserve the autonomy of human intervention in the decision-making process.

7.2 Decisions based on the results provided by Big Data analytics should take into account all the circumstances concerning the data and not be based on merely de-contextualised information or data processing results.

7.3 Where decisions based on Big Data might affect individual rights significantly or produce legal effects, a human decision-maker should, upon request of the data subject, provide her or him with the reasoning underlying the processing, including the consequences for the data subject of this reasoning.

7.4 On the basis of reasonable arguments, the human decision-maker should be allowed the freedom not to rely on the result of the recommendations provided using Big Data.

7.5 Where there are indications from which it may be presumed that there has been direct or indirect discrimination based on Big Data analysis, controllers and processors should demonstrate the absence of discrimination.

7.6 The subjects that are affected by a decision based on Big Data have the right to challenge this decision before a competent authority."

[1] Vgl. Albrecht/Jotzo (2017), S. 39.
[2] Vgl. Spindler/Thorun (2016), S. 2.
[3] Mit Art. 97 DS-GVO sieht der Gesetzgeber eine regelmäßige Überprüfung/Bewertung der DS-GVO vor: Bis zum 25. Mai 2020 und danach alle vier Jahre hat die Kommission dem Europäischen Parlament und dem Rat regelmäßig einen Evaluationsbericht vorzuglegen.
[4] Vgl. Council of Europe (2017), S. 5

Wie die oben genannten Grundsätze praktisch wirksam werden sollen, bleibt letztendlich offen, wenn a) unklar bleibt, wie die geforderte Beweislastumkehr (siehe 7.5) bei gerichtlichen Auseinandersetzungen faktisch wirksam werden soll bzw. b) „Codes of Conduct" und „Audits/Zertifizierungen" optional bleiben und nicht – wie etwa in der Schweiz für gewisse Anwendungen mit Gesundheitsdaten – zwingend gesetzlich vorgeschrieben sind.[5] Von einer gesetzlich verankerten privatwirtschaftlichen datenschutzrechtlichen Pflichtprüfung (in Analogie zur Prüfung von Jahresabschlüssen durch privatwirtschaftliche Wirtschaftsprüfer) scheint das Datenschutzrecht, trotz seiner hohen Brisanz in der modernen Informationsgesellschaft, noch weit entfernt zu sein. Auch steht die theoretische Durchdringung freier Märkte privatwirtschaftlicher Prüfanstalten, auf denen sich zu begutachtende Unternehmen ihre Gutachter frei wählen können (und kritische Gutachter damit u. U. im Sinne einer „adverse selection" systematisch aussortiert werden könnten), hinsichtlich seiner Angemessenheit und Gesamteffektivität noch aus. Inwiefern DS-GVO-Zertifikate und sonstige Nicht-DS-GVO-Zertifikate sowie IT-Sicherheitszertifikate zu einer unübersichtlichen und verwirrenden Siegelvielfalt für den Verbraucher führen könnten, ist zum jetzigen Zeitpunkt unklar und schwer abzusehen. Als sozio-technisches System ist insgesamt aber auf eine umfassende Evaluierung und Zertifizierung von Big-Data-basierten IuK-Systemen wert zu legen. Das heißt: Nicht nur die Datenverarbeitung und die verwendeten Algorithmen sind zu auditieren, sondern v. a. auch die Technikverwender, deren Geeignetheit, Training im Umgang mit den Systemen und Wissen um die Möglichkeiten und Grenzen der Systeme. Die Markt- und Meinungsforschung, die sich selbst als wissenschaftliche Unternehmung verstehen will und stark gegenüber der Direktwerbung abgrenzt[6], sollte nicht ein antiquiertes Wissenschaftsbild konservieren und der Ansicht erliegen, mit ihren Big-Data-basierten Statistiken und Vorhersagen zweckfreie Erkenntnisse zu produzieren, die keine Effekte für Individuen zeitigen.[7] Die Einführung eines Sammelklagerechts (in Verbindung mit dem existierenden Verbandsklagerecht) dürfte deshalb eine adäquate Erweiterung des allgemeinen Governance-Rahmens in Zeiten von Big Data darstellen, um der zunehmenden statistischen Beurteilung von Menschen in ad-hoc-Gruppen und davon ausgehenden potentiellen Diskriminierungsphänomenen Herr werden zu können. Der Staat könnte sich hinsichtlich potentiell diskriminierender Effekte von Big-Data-Analytics ferner die Expertise der Wettbewerber zunutze machen: Martini plädiert deshalb dafür, dass der Gesetzgeber die Abmahnbefugnisse der §§ 12 Abs. 1 Satz 1, 8 Abs. 3 Nr. 1, Abs. 1 i.V. mit § 5 Abs. 1 Satz 1 und 2 Nr. 6 UWG bzw. i.V. mit § 3 Abs. 3 UWG um den Tatbestand diskriminierender oder persönlichkeitsverletzender Softwareanwendungen erweitert.[8] Ferner sollte – so Martini – auch das Verbandsklagerecht derart erweitert werden, dass gegen diskriminierende algorithmische Entscheidungsfindungen vorgegangen werden kann.[9] Auch scheint die Stellschraube „Reichweite der Rechtskraft zivilgerichtlicher Urteile" vielversprechend, etwa indem der Gesetzgeber eine Rechtskrafterstreckung verfügt.[10] Insgesamt scheint auch die Stärkung des Schutzes von Whistleblowern als auch einer investigativen Presse angebracht, bedenkt man, dass eine Vielzahl von den in den Medien und Wissenschaften diskutierten negativen Effekten von Big Data genau aus diesen Quellen stammen. Eine verstärkte wissenschaftliche Begleitforschung von Big-Data-Analytics ist zudem unabdingbar. Für manche Betrachtungsbereiche, wie etwa dem Predictive Policing, mag diese Forschung einfach möglich sein. In anderen Betrachtungsbereichen ist der Zugang zum Forschungsobjekt jedoch verstellt, weil geschäftliche Geheimhaltungsinteressen dem grundsätzlich entgegenstehen (etwa bei der Erforschung sozialer Medien oder den Strukturen und Praktiken der Datenindustrie). Dies zeigt: Big-Data- und Algorithmenregulierung bewegen sich in einem komplexen Spannungsverhältnis von Persönlichkeitsschutz, Schutz von Betriebs- und Geschäftsgeheimnissen und der

[5] Vgl. Lachaud (2016), S. 825.
[6] Vgl. Hornung/Hofmann 2017, S. 3.
[7] Zur Unhaltbarkeit des anachronistischen Wissenschaftsverständnisses einer vermeintlich zweckfreien Wissenschaft vgl. Lenk (2001).
[8] Vgl. Martini (2017), S. 1024.
[9] Vgl. Martini (2017), S. 1024.
[10] Zu den Details vgl. Martini (2017), S. 1025.

Förderung digitaler Wertschöpfungspotentiale.[11] Je weiter Big Data und die automatisierte Verarbeitung personenbezogener Daten in all unsere Lebensbereich vordringt, desto wichtiger wird es, dass der rechtwissenschaftliche Diskurs nicht bei der datenschutzrechtlichen Innenbetrachtung stehen bleibt, sondern –– etwa hinsichtlich Datenmacht und Unternehmensfusionen – auch andere Rechtsgebiete wie das Kartellrecht, das Verbraucher(schutz)recht und das AGB-Recht in den Blick nimmt, um den Gesamtregelungsrahmen effektiv und effizient zu gestalten.[12]

[11] Vgl. Martini (2017), S. 1019.
[12] Vgl. Lewinski/Herrmann (2017a); Lewinski/Herrmann (2017b).

Literaturverzeichnis

Albrecht, Jan Philipp; Jotzo, Florian (2017): Das neue Datenschutzrecht der EU. Grundlagen – Gesetzgebungsverfahren – Synopse. Nomos.

Barocas, Solon; Nissenbaum, Helen (2014): Big Data's End Run around Anonymity and Consent. In: Lane, Julia et al. (Hrsg.): Privacy, Big Data, and the Public Good. Cambridge University Press. S. 44-75.

BMJV (2015): One-Pager – Muster für transparente Datenschutzhinweise. http://www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html

Borgesius, Frederik (2016): Singeling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. In: Computer Law & Security Review, Vol. 32, S. 256-271.

Borgesius, Frederik; Poort, Joost (2017): Online Price Discrimination and EU Data Privacy Law. In: Journal of Consumer Policy, Vol. 40, S. 347-366.

Council of Europe (2017): Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. https://rm.coe.int/16806ebe7a

Culik, Nicolai; Döpke, Christian (2017): Zweckbindungsgrundsatz gegen den unkontrollierten Einsatz von Big-Data-Anwendungen. In: Zeitschrift für Datenschutz – ZD, Heft 5, S. 226-230.

De Hert, Paul; Papakonstantinou, Vagelis (2016): The new General Data Protection Regulation: Still a sound system for the protection of individuals? In: Computer Law & Security Review, Vol. 32, S. 179-194.

Engeler, Malte (2017): Das überschätzte Kopplungsverbot. In: Zeitschrift für Datenschutz – ZD, Heft 2, S. 55-62.

Haag, Niels Christian (2016): EU-Datenschutz-Grundverordnung – Die Rolle der Aufsichtsbehörden. https://www.datenschutzbeauftragter-info.de/eu-datenschutz-grundverordnung-die-rolle-der-aufsichtsbehoerden/

Hornung, Gerrit; Hofmann, Kai (2017): Die Auswirkungen der europäischen Datenschutzreform auf die Markt- und Meinungsforschung. In: Zeitschrift für Datenschutz – ZD, Beilage 4/2017.

Kettner, Sara Elisa; Thorun, Christian; Vetter, Max (2018): Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz.
https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf

Kolany-Raiser, Barbara; Heil, Reinhard; Orwat, Carsten; Hoeren, Thomas (2018): Big Data und Gesellschaft: eine multidisziplinäre Annäherung. Springer.

Kosow, Hannah; Gaßner, Robert (2008): Methoden der Zukunfts- und Szenarioanalyse. Überblick, Bewertung und Auswahlkriterien. WerkstattBericht Nr. 103. Institut für Zukunftsstudien und Technologiebewertung IZT. https://www.izt.de/fileadmin/publikationen/IZT_WB103.pdf

Kuner, Christopher; Svantesson, Dan; Cate, Fred; Lynskey, Orla; Millard, Christopher (2017): Machine learning with personal data: is data protection law smart enough to meet the challenge?, In: International Data Privacy Law, Vol. 7, Issue 1, S. 1-2.

Lachaud, Eric (2016): Why the certification process defined in the General Data Protection Regulation cannot be successful. In: Computer Law & Security Review, Vol. 32, S. 814-826.

Lenk, Hans (2001). Wissenschaft und Ethik. Reclam.

Lewinski, Kai von; Herrmann, Christoph (2017a): Vorrang des europäischen Datenschutzrechts gegenüber Verbraucherschutz- und AGB-Recht. Teil 1: Materielles Recht. In: PinG – Privacy in Germany, Heft 5, S. 165-172.

Lewinski, Kai von; Herrmann, Christoph (2017a): Vorrang des europäischen Datenschutzrechts gegenüber Verbraucherschutz- und AGB-Recht. Teil 2: Aufsichtsbehörden. In: PinG – Privacy in Germany, Heft 6, S. 209-216.

Liebert, Wolfgang (2013): Dual-Use-Forschung und –Technologie. In: Grunwald, Armin (Hrsg.): Handbuch Technikethik. J.B. Metzler. S. 243-248.

Martini, Mario (2017): Algorithmen als Herausforderung für die Rechtsordnung. In: JuristenZeitung JZ, Heft 21, 72. Jahrgang, S. 1017-1072.

Mittelstadt, Brent; Allo, Patrick; Taddeo, Mariarosaria; Wachter, Sandra; Floridi, Luciano (2016): The ethics of algorithms: Mapping the debate. In: Big Data & Society, July-December 2016, S. 1-21.

Moos, Flemming; Rothkegel, Tobias (2016): Nutzung von Scoring-Diensten im Online-Versandhandel. Scoring-Verfahren im Spannungsfeld von BDSG, AGG und DS-GVO. In: Zeitschrift für Datenschutz – ZD, Heft 12, S. 561-568.

Paal, Boris; Pauly, Daniel (2017): Datenschutz-Grundverordnung. Kommentar. C.H. Beck.

Pentland, Alex (2014): Social Physics. The Penguin Press.

Roßnagel, Alexander (2013): Big Data -- Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. In: Zeitschrift für Datenschutz – ZD, Heft 11, S. 562-567.

Roßnagel, Alexander; Geminn, Christian; Jandt, Silke; Richter, Philipp (2016): Datenschutzrecht 2016 – „Smart“ genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts. Kassel University Press.

Schulzki-Haddouti, Christiane (2017): Prüfungs-Placebo. Datenschutzbehörden tun sich mit technischen Prüfungen schwer. In: c't, Heft 19, S. 120-122.

Simitis, Spiros (1990): „Sensitive Daten“ -- Zur Geschichte und Wirkung einer Fiktion. In: Brem, Ernst et al. (Hrsg.): Festschrift zum 65. Geburtstag von Mario M. Pedrazzini, Verlag Stämpfli & Cie AG Bern, S. 469-493.

Specht, Louisa (2017): Das Verhältnis möglicher Datenrechte zum Datenschutzrecht. In: GRUR Int. – Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil, Heft 12, S. 1040-1047.

Spindler, Gerald; Thorun, Christian (2016): Die Rolle der Ko-Regulierung in der Informationsgesellschaft. Handlungsempfehlungen für eine digitale Ordnungspolitik. In: MMR - MultiMedia und Recht. Zeitschrift für Informations-, Telekommunikations- und Medienrecht, Beilage 6/2016.

Steinmüller, Karlheinz (1997): Grundlagen und Methoden der Zukunftsforschung. Werkstattbericht 21. Sekretariat für Zukunftsforschung. http://steinmuller.de/media/pdf/WB%2021%20Grundlagen.pdf

Stiftung Datenschutz (2018): Praktische Umsetzung des Rechts auf Datenübertragbarkeit: Rechtliche, technische und verbraucherbezogene Implikationen. Zusammenfassung und Handlungsempfehlungen. https://stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/kurzversion_studie_datenportabilitaet.pdf

Türpe, Sven; Geuter, Jürgen; Poller, Andreas (2016): Emission statt Transaktion: Weshalb das klassische Datenschutzparadigma nicht mehr funktioniert. In: Friedewald, Michael; Lamla, Jörn; Roßnagel, Alexander (Hrsg.): Informationelle Selbstbestimmung im digitalen Wandel. Springer-Vieweg.

ULD / GP Forschugsgruppe (2014): Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen. https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Scoring-Studie.pdf?__blob=publicationFile&v=3

Wachter, Sandra; Mittelstadt, Brent; Floridi, Luciano (2017): Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. In: International Data Privacy Law, Vol. 7, Issue 2, S. 76–99.

Weichert, Thilo (2014): Scoring in Zeiten von Big Data. In: ZRP – Zeitschrift für Rechtspolitik, Heft 6, S. 168-171.

Weichert, Thilo (2017): „Sensitive Daten“ revisited. In: DuD Datenschutz und Datensicherheit, Heft 9, S. 538-543.

Zarsky, Tal (2017): Incompatible: The GDPR in the Age of Big Data. In: Seton Hall Law Review, Vol. 47, No. 4, S. 995-1020. https://ssrn.com/abstract=3022646

KIT Scientific Working Papers
ISSN 2194-1629

www.kit.edu